==========

H I P A A L E R T Volume 3, Number 2 February 26, 2002

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

==========
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total nearly 16,000.

IF YOU LIKE HIPAALERT, YOU'LL LOVE WWW.HIPAADVISORY.COM! -- Phoenix' "HIPAA Hub of the Web"
==========

T H I S I S S U E

==========

COMING UP IN TWO DAYS:

"Getting Something Back: Finding Real Value in Your HIPAA Privacy Implementation"
Audio Conference presented by Tom Grove, Director, Phoenix Health Systems,
Thursday, February 28, 2:00 - 3:00 p.m. EST

For more info or to sign up, visit our HIPAAstore!
http://www.hipaadvisory.com/ezcart/index.cfm?tt226

Other outstanding HIPAA Audioconferences and tapes are also available.

==========

1 >> F R O M T H E E D I T O R S:

In the past, healthcare organizations confronting change have fended for themselves more often than not. "Pulling together" has a nice ring to it, but converting the concept into reality has been hampered by marketplace concerns, divergent priorities, and perhaps a certain parochialism.

The HIPAA revolution continues to spark more healthcare community efforts to share knowledge and work together than we have ever seen. Taking advantage of the Internet's extraordinary enabling power, groups within states, across states, and across the industry are joining together to share experiences, concerns and solutions. The list of collaborative intitiatives is long...a sampling includes WEDI-SNIP, NCHICA, SHARP, CHITA, CoSNIP, CALINX, HARK, MAHI, MHDC, NESCO, NEHEN, NYHUG, HIPAA GIVES, and even a HIPAA COW (HIPAA Collaborative Wisconsin).

Our February HIPAAlert focuses on and celebrates HIPAA collaboration. This issue is, itself, an example of the best kind of HIPAA knowledge-sharing: experiences, ideas and expertise freely offered by six busy, but concerned, industry thinkers. Our thanks, and kudos to: Roy Rada, Kepa Zubeldia, DeDee Birdsall, Steve Fox, Rachel Wilson, and Eric Maiwald for their outstanding contributions!

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall, Director of Internet Services
bhall@phoenixhealth.com

==========

2 >> H I P A A n e w s

*** HIMSS Leadership Survey Reports HIPAA is Industry's Highest Priority ***

The Annual HIMSS Leadership Survey for 2002 reports that over 80% of respondents expect that HIPAA compliance will remain the biggest issue facing them over the next two years. Reducing medical errors (52%) and cost pressures (51%) are reported to be the number two and three most pressing issues. The Healthcare Information and Management Systems Society (HIMSS) conducted the survey, sponsored by Superior Consultant Company.

Read the report:
http://www.hipaadvisory.com/news/index.htm#0225himrep

*** Bush 2003 Budget Proposes Over $60 Million for HIPAA ***

President Bush's proposed budget for FY 2003 includes $64.1 million for Administrative Simplification activities:

-- $9.6 million to ensure that the Centers for Medicaid and Medicare Services (CMS), as a health plan, is compliant with the Transaction Rule standards by October 2003
-- $10 million to conduct testing with Medicare providers to ensure that they submit HIPAA-compliant claims
-- $10 million to conduct outreach and education efforts with providers, States (including Medicaid programs) and other CMS partners
-- $34.5 million to complete the development of, and begin operation of, a system to assign identifiers to health plans and providers

The HIMSS Advocacy Dispatch of February 18, 2002 notes that these figures are part of a proposal that doesn't yet represent actual funding, but that is proceeding through the Federal budget process. At present, no funding is dedicated to Administrative Simplification activities except for the $44.2 million authorized in the recent Administrative Simplification Compliance Act that allowed for a one-year extension on the Transaction Standards rule. In order to have other dedicated HIPAA funding for the current fiscal year, Congress would need to pass a supplemental appropriations bill. The Coalition for Health Information Policy (CHIP), of which HIMSS is a part of, has been asked to help justify the urgent need for those dollars this year.

Read more: http://www.hipaadvisory.com/news/index.htm#0225himss

*** AHA to HHS: Change Privacy Regs & Standardize HIPAA Code Sets ***

AHAnews reports that the American Hospital Assocation (AHA) joined 88 other health care organizations to voice concern over what impact HIPAA's final privacy regs might have on health-related research. In a letter sent to HHS Secretary Tommy Thompson last week, the group said the standard for de-identifying medical information would essentially render some data useless for research purposes. They proposed that the standards be modified to limit it to direct identifiers. AHA also recently recommended in testimony before the National Committee on Vital Health Statistics' Subcommittee on Standards and Security (NCVHS) and in a previous letter to HHS Secretary Thompson that the medical code sets for transactions under HIPAA be updated no more than annually and on the same date by all covered entities.

Read more: http://www.hipaadvisory.com/news/recentnews.htm#0213aha

*** House Passes Computer Security Bill ***

Congress overwhelmingly approved a bill February 7th that offers $880 million in funding to government agencies for researching ways to improve U.S. computer and network security. The House voted 400-12 in favor of HR 3394, the Cyber Security Research and Development Act, sponsored by Science Committee Chairman Sherwood Boehlert, (R-NY). The $880 million would be split between the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) for use in Cybersecurity research efforts. The bill has been referred to the Senate Committee on Commerce, Science, and Transportation.

Read more: http://www.hipaadvisory.com/news/recentnews.htm#0211wp

==========

3 >> H I P A A v i e w: The Question of HIPAA "Best Practices"
by Roy Rada, M.D., Ph.D.

THE PROBLEM:

Over 20% of healthcare organizations say that they are adopting a "best practices" approach to HIPAA, according to the most recent national HIPAA survey by Phoenix Health Systems and HIMSS (January 2002). Increasingly, healthcare professionals with HIPAA responsibility want to know what practices are "best." How should we determine what is best? In efforts to uncover HIPAA best practices developed by our peers, it's not uncommon to learn that the so-called "best" practices don't pass muster after careful scrutiny or efforts to duplicate their originators' success.

HIPAA's relatively short life has provided little time or opportunity for the refinement or maturation of compliance methodologies. Within the HIPAA compliance arena, inexperience is more common than experience; further, methodology development and implementation time is limited by fast-approaching Federal deadlines. Short of inventing one's own HIPAA wheel, how can we uncover the best HIPAA practices to adapt to our enterprise's needs?

IS SHARING ENOUGH?

Sharing information about our practices implies only that the information owners have enough confidence in their tools and techniques that they are willing to have others view them. The methodologies cannot be judged as "best practices," simply because they were effective for the originators and are attractive to the borrowers.

However, when a number of people borrow or adapt a practice, it can be argued that it becomes a "common practice." Does it follow that a "best practice" will be the end result of this iterative process? Common practice evolves as often from expediency or other business survival considerations as from someone's far-reaching vision or a desire for excellence or elegance. One way to identify good practices is to gather knowledgeable, objective experts and common practices, and have the experts weed through the common practices and suggest which ones are good. If the organizers of this activity would publish the results, then all might benefit.

Some of this is occurring. WEDI-SNIP's work in this direction is notable. So are the collaborative initiatives of NCHICA, SHARP, AHIMA, and the Academic Medical Centers, which have produced a variety of practice guidelines and methodology tools. Even some vendors and consultants have freely shared useful materials - laudable even if one underlying reason is to attract business.

But, this spirit of sharing is by no means universal. A senior officer of a major Mid-Atlantic healthcare delivery systems explains: Everyone must become HIPAA-compliant, so achieving compliance presents no competitive advantage. However, an organization may gain a competitive advantage if (for example) it has COST-EFFECTIVELY developed HIPAA compliance programs. Organizations don't want to reduce this advantage by sharing the knowledge that generated it. An executive with a national healthcare network differently expresses some organizations' reluctance to share methodology information, noting that such sharing might make them more susceptible to law suits.

Jurying, or lack of it, should also be noted as a factor to be aware of when considering adopting either a "common" practice or a claimed "best" HIPAA practice. Inadequate review and evaluation is probably a factor in the general dearth of available best practices information. Even where healthcare professionals from non-profit or for-profit organizations have joined together to identify or promulgate so-called best practices, little data is made available to verify the quality or value of the offered solutions. Where are case study results, reviews or analyses of the practices and tools, structured around valid (or at least, reasonable) criteria?

Before considering any practice "best" or "good," it should, for example, have been fully deployed and have produced demonstrable results that meet HIPAA requirements and the practice's objectives. Efficiency of the practice in terms of dollars, time and other resource costs should be an important factor. The practice should have the potential for wide application or adaptability. Further, the results and benefits of the practice should have been documented and measured to determine if and how they exceed benchmarks.

NEXT STEPS?

Perhaps an established and widely respected advisory body - such as the National Committee on Vital and Health Statistics (NCVHS) - should become the "center" of an industry-wide effort to develop public repositories of "best practices." NCVHS is the statutory public advisory body to HHS in the area of health data, and its 18-member committee serves as a forum for regular interaction with healthcare private sector groups. Members are leaders in such areas as electronic data interchange, privacy and security, public health, purchasing/financing health care services, health information systems, health services research, consumer interests in health information, health data standards, and the provision of health services.

A feature of the recent Administrative Simplification Compliance Act -- which provides for an extension of the Transactions and Code Sets Rule compliance date to covered entities that file a compliance plan -- provides the germ of this concept: "The Secretary of Health and Human Services shall furnish the National Committee on Vital and Health Statistics (NCVHS) with a sample of the plans submitted ... NCVHS shall analyze the sample of the plans furnished (and) shall regularly publish, and widely disseminate to the public, reports containing effective solutions to compliance problems. Such reports shall not relate specifically to any one plan but shall be written for the purpose of assisting the maximum number of persons to come into compliance by addressing the most common or challenging problems encountered." NCVHS is in a good position to help collect, fine-tune and publish useful HIPAA approaches, practices and tools. It is also in a good position to develop standard criteria for evaluating them, and to drive their review by NCVHS members and other qualified volunteers. At least three caveats are in order:

-- NCVHS has been mandated by the Act only to assess and report on Transactions and Code Sets compliance plans submitted by covered entities. Privacy and security-related practices might also be evaluated by NCVHS, perhaps through its Privacy and Confidentiality subcommittee. In all cases, it will be important to apply specific, standard criteria to any practices under review.

-- What will constitute good practice for one type of entity, like a solo-physician practice, is likely to be different from what will constitute good practice for a 50-hospital network. Where appropriate, producing scalable versions of good practices would be an ideal approach. Otherwise, good practices may need to be identified by entity-type.

-- The value of a repository of good practices will be high, if and only if, the repository is comprehensive, readily accessible and properly maintained and updated across time.

NCVHS has recognized the importance of identifying 'good practices' in helping the industry efficiently comply with HIPAA. While NCVHS is not

resourced to single-handedly identify all good practices, it should begin to actively interpret the findings it collects in a way that helps distinguish those practices that the Committee believes are 'good'. More importantly, the Committee should recommend to HHS the ways that the government can help coordinate wider efforts to share common practices and work toward best practices.

Roy Rada, M.D., Ph.D., is Professor, Health Care Information Systems, University of Maryland, Baltimore County, and a frequent industry speaker on HIPAA-related issues.

==========

4 >> H I P A A c t i o n: Shaping Up Your Business Associates -- A Case Study on Compliance and Better Relationship Management
by DeDee Birdsall

Do you know who your Business Associates are? According to HIPAA, a Business Associate is "a person who performs a function or activity on behalf of a covered entity." Examples are lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms and billing firms. Your Business Associate can also be a covered entity; however, Business Associates are not members of your workforce.

According to the Privacy regulation, if you're a covered entity, it's your job to require that all Business Associates comply with the law, as well as any agents or subcontractors thereof. With all that said, who really qualifies as a true Business Associate? How do you locate and understand all the relationships in place in your organization? Is there one person who holds the key? Does a repository of information exist? Do you have dedicated staff for managing these relationships? In our organization, the answer to most of these questions is no.

So where do you begin and what must you consider? In our organization's attempt to tackle Business Associates, we identified methods for logically breaking down this process into more manageable pieces and have been steadily working at the process for several months. Hopefully, this document will provide some insight into one method for complying with all privacy laws and building and maintaining better Business Associate relationships.

BUILDING THE PROJECT TEAM AND SETTING DIRECTION

Our Business Associate project team was organized and includes the privacy officer, HIPAA project manager, technical writers, corporate counsel and various administrative personnel. The team is responsible for interpreting the law, defining goals related to Business Associates, creating

task lists and timelines and moving the project forward.

Through discussions regarding current processes we determined that an inventory of our Business Associates was necessary and if possible, the information should be captured and stored in an online database. Creating a central database of easily accessible Business Associate information would be a strong foundation for improving our processes regarding third-party relationships. Technical staff was added to the project team to develop the database template for all Business Associates. The overall goal with the database was to provide one-stop shopping for all our Business Associate information.

The finished database template contains fields to identify historical accounts of all relationships including details regarding contract and customer ownership; contract terms; amendment history; relationship and compliance summaries; and various attributes related to the relationship. Plans for scanning physical contracts and amendments were also approved and processes were identified for creating linked PDF files. The template was created and approved, and provided the direction for conducting the inventory.

CONDUCTING THE INVENTORY AND BUILDING THE DATABASE

The next step in the process was to begin the Business Associate inventory. Technical writers were assigned to this function and began by working with our legal department to do an initial review of current contract processes and obtain reports detailing Business Associates. In theory, this seemed to be a straightforward task; however, the database template was much more specific than information that historically had been kept on Business Associates. With the recent influx of privacy laws, we made the decision to rebuild the files and to provide more detail than in the past. So, as you can see below, our inventory task became much more difficult than originally anticipated and required extensions to the original project timelines.

The following steps encompass the inventory portion of the project that are currently underway. We anticipate the inventory and database project will continue ongoing throughout the life of the project.

* Draft a definition of Business Associates as related to the Gramm-Leach-Bliley Act (privacy of non-public information) and HIPAA.
* Create a list of current Business Associates from legal department files or through interviews with contract relationship managers.
* Locate and record all in-house contract relationship managers.
This is an important step in understanding the relationships. Without in-house ownership attached to the contracts, it is difficult to understand and document the relationship.
* Locate missing Business Associates, or relationships that have been established outside the corporate contract process, by producing accounts

payable reports by cost center for the past year.
* Eliminate obvious payees including charitable and professional organizations. Research questionable payees that fall within the structure of the database.
* Update the database with missing Business Associate information.
* Provide contract relationship managers with procedures and definition for determining the relationship status of each partner (Business Associate or non-Business Associate in regards to Gramm-Leach-Bliley and HIPAA).
* Code all contracts on the database to indicate relationship status.
* Interview contract relationship managers to capture information for the database.
* Document relationship summaries and populate the database for each Business Associate. (The database includes fields to hold names, addresses, contract details such as length of term, amendment history, type of contract, summary of the relationship, products the contract supports, and compliance summaries).
* Scan all contract files to PDF files and attach to the appropriate Business Associate file in the database.
* Create programs to pull all Business Associate names and addresses for auto mailing of the Confidential Information Agreement and auto-generated cover letter.
* Verify all Business Associate information is accurately entered to the database.

UPDATING CONTRACTS

Updating existing contracts and changing procedures for establishing new Business Associate relationships was started shortly after the research task began. The project team was broadened to include outside counsel, executive management, and steering committee members. Many questions were raised regarding the approach to take, i.e., what type of agreement to have. We weighed the pros and cons of having separate contracts in support of the chain of trust, trading partner, and Business Associate agreement, or having one contract to incorporate these along with the agreement required by Gramm-Leach-Bliley for the confidentiality of non-public information. Timeframes for compliance were also examined and the team made the decision to attempt one agreement by the July 1, 2002, Gramm-Leach-Bliley compliance date.

The result was a single Confidential Information Agreement that reflects our company's commitment to maintain the confidentiality of information it has developed, or has been entrusted to it. The agreement states our company's obligation to keep information confidential arises from various laws, regulations, contractual commitments and company policy. This agreement when accepted by both parties will become an addendum to the original contract for all existing Business Associates and will satisfy compliance requirements for both laws. The agreement will also become a part of new Business Associate relationships as they're established. The agreement is

easy to understand, and clearly identifies three separate privacy issues.

* Confidentiality of Health Information
* Personally Identifiable Financial Information
* Business Confidential Information (covers proprietary information)

Although our Business Associate agreement is still in the draft stage, we believe once approved by the project team, it will serve all purposes under Gramm-Leach-Bliley and HIPAA and will protect our proprietary information.

In addition, new procedures are being developed for in-house relationship managers to facilitate discussions with new Business Associates if we are unable to reach agreement on the terms and conditions of the Confidential Information Agreement.

The steps involved in updating existing contracts include:

* Develop and obtain approval of Confidential Information Agreement.
* Create an automated address file from Business Associate database.
* Develop Business Associate cover letter explaining agreement.
* Develop a follow-up letter and auto generation if no response received in 30 days.
* Develop internal automated processes for generating the cover letter and all subsequent follow-up letters.
* Mail agreements to all Business Associates.
* Develop a process for receiving and recording returned mail and signed responses.
* Develop a process for negotiating contractual language with Business Associates.
* Develop an automated process for audit trail on the database to indicate mailing and acceptance dates.
* Scan all signed contracts and link to appropriate Business Associate file on the database.
* Complete database fields related to compliance for Gramm-Leach-Bliley and HIPAA.

IMPLEMENTING NEW PROCESSES

With research and implementation underway, we found it was time to consider new processes for maintaining better relationships with our Business Associates. Through project definition and task lists, we have been able to easily establish these processes. Once refined, they will be presented to the HIPAA steering committee and executive management for review and approval with implementation in 2002. The following tasks represent new process ideas. It is anticipated that this list will continue to grow as work continues on the overall project.

* Define responsibility for maintenance of the database and all third-party

relationships. Determine if dedicated staff exists or a contract administrator is required.
* Define contract control procedures by documenting processes required by all in-house contract relationship managers to complete a thorough and consistent contract review before a contract is signed or renewed. Steps to be considered include guidelines for reviewing basic contract provisions for such things as termination, mutual indemnification, confidentiality, exclusivity, reciprocity, and attention to all state laws.
* Create process by which authorized staff review and approve all pending contracts. Applicable parties should include staff from corporate financial, executive, and legal.
* Publish and maintain a list of qualified contract signers/in-house relationship managers.
* Establish procedures for the contract administrator or dedicated staff to build and maintain relationship files in the database as new relationships are formed and existing relationships are renewed.
* Develop reports to flag renewals, terminations, and missing relationship information.
* Establish annual review procedures for existing contracts and relationships. Work with in-house relationship managers to verify all information is accurate.
* Establish procedures for contract termination and file archiving on the database.

MAINTAINING RELATIONSHIPS AND MEETING COMPLIANCE REQUIREMENTS

Overall, when it comes to maintaining Business Associate relationships, we now believe we should be able to easily answer these questions:

* Do we understand the term "Business Associate" as it relates to privacy laws?
* Do our Business Associate contracts comply with all privacy laws?
* Do we have auditing procedures in place to assure compliance?
* Do we have dedicated staff to manage third-party relationships and Business Associates?
* Do we have a repository of information regarding all third-party relationships and Business Associates?
* Do we have procedures in place for interacting with third parties on a regular basis?
* Do we have procedures in place for establishing new relationships and maintaining existing relationships?

If the answer to any of these questions is "no," it's time to review our practices, revisit the project plan, assign resources, and complete the unfinished tasks. The answer must be yes to move forward.

When we look at this project, we see HIPAA as a means for helping us define procedures for making us better third-party relationship managers.

As with many projects related to HIPAA, they just make good business sense! However, given the compliance date and the number of projects, most companies are not equipped to manage so many "good practice projects" in the same year. Good luck and we hope this is helpful for those of you in the early stages of defining your Business Associate project.

DeDee Birdsall is an Assistant Vice President at American Republic Insurance Company and serves as its HIPAA Project Manager. American Republic Insurance Company offers a variety of major medical, Medicare supplement, life, annuity and critical care/cancer care products.

==========

5 >> H I P A A / LAW : Legal Q/A
"Writing Business Associate Contracts"
by Steve Fox, Esq., & Rachel Wilson, Esq.

Q. We're starting to look at our Business Associates. What should we consider when developing the Business Associate contracts required by HIPAA?

A. It's not too soon to incorporate HIPAA's Business Associate requirements into contracts with existing vendors or to open a dialogue about the requirements during negotiations with potential vendors, and include relevant provisions in resulting contracts.

HIPAA's Privacy Regulation requires covered entities to obtain satisfactory assurance that their Business Associates will "appropriately safeguard" protected health information ("PHI"). These assurances must be documented in a written contract or other written agreement with the Business Associate. There are three elements essential to obtaining the required assurances.

First, contracts should include, or make specific reference to, the Business Associate contract terms set forth in the Privacy Regulation, particularly those terms related to the Business Associate's use and disclosure of PHI. Contracts should also include concrete examples, performance criteria, or the standard of care required to satisfy the corresponding HIPAA requirement. For example, under the Privacy Regulation, Business Associate contracts must provide that Business Associates will use appropriate safeguards to prevent the use or disclosure of PHI in any manner not set forth under the agreement. Because the actions of Business Associates (as they relate to the use and disclosure of PHI) are considered to be the actions of the covered entity that engaged them, it is imperative that the contracts define a minimum standard of performance that, if met, will constitute an "appropriate safeguard." This is also important because covered entities have an obligation to disclose their privacy practices to patients. It will be

difficult to prepare a Notice of Privacy Practices without an understanding of, and comfort level with, the safeguards implemented by a Business Associate.

Second, Business Associate contracts must contemplate future amendment and modifications. Business Associates should agree, by way of example, that if:

-- the Privacy Regulation is modified by Congress or HHS, or is interpreted by a court in a manner impacting compliance, or

-- there is a material change in the business practices and procedures of the covered entity,

then the Business Associate contract may be amended. This puts the Business Associate on notice that the agreement is a living document which may evolve during the course of performance.

Finally, a covered entity must have the unilateral right to terminate a Business Associate contract if it determines that the Business Associate has violated a material term of the contract. This remains one of the most difficult areas of negotiation with vendors. However, since covered entities are subject to sanctions if they have knowledge of a Business Associate's wrongful activity and fail to take reasonable steps to have the breach cured, this is an essential term in every Business Associate contract. If a covered entity is unable to effect a cure, it must either terminate the contract or report the problem to HHS.

Read past HIPAA Legal Q/A articles:
http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton LLP. http://www.pepperlaw.com/
Disclaimer: This information is general in nature and should not be relied upon as legal advice.

==========

6 >> H I P A A / EDI: Q/A on Transactions & Code Sets
"What's Happening to Local Codes?"
by Kepa Zubeldia, M.D.

Q. I understand the HCPCS "local" codes are going away. When will those rules come out, and how can I get ready?

A. Actually, the process is well under way. There are no "rules" to be

published in the Federal Register for this code migration, but a much simpler method. Before we look at how the migration is happening, let's review the history of the "local" codes.

In the beginning there were "Relative Value" codes, and they were good. But each state had their RV codes, and it was very difficult to bill across state lines. So the AMA said: let's build a coding structure that can be used for billing on a national basis. And it was done. And they were called "Common Procedural Terminology" (CPT) codes. And they were very good.

So, the states and Medicare adopted the CPT in the late 70s and early 80s. However, the CPT only reflected the "medical" procedures, leaving out all sorts of other reimbursable products and services that were of interest to Medicare and Medicaid. So, rather than going back to the RV codes, HCFA (now CMS) designed a "supplement" to the CPT, to accommodate all those additions on a national basis. And thus the Level-II HCPCS were born. Level-I are the CPT themselves, and Level-II the national HCPCS codes. Since the states had a plethora of state specific programs that did not lend themselves to national codes, the HCPCS accommodated a Level-III coding system. These Level-III codes were to be also registered with HCFA, and given the initial letters of W, X, Y, and Z. However, the process to obtain these registered Level-III codes was a simple one, not requiring proof of national use of the code, just the need by a particular state. These codes were called "Local" HCPCS codes, as opposed to the "National" codes in Level-II.

No matter how easy the registration process, most Level-III codes were never registered with HCFA, but just issued by the states based on their particular needs. In fact, not only the states, but some payers also felt free to issue their own unregistered codes starting with the last few letters of the alphabet.

Why did they need additional codes? Some times it would be to designate a specific place of service that had higher reimbursement rates. Other times it could be for a particular pilot project or experimental program. Or perhaps to indicate a special contract or pricing arrangement with a group of providers. Or some state-mandated program that had specific conditions of participation. Or a multitude of other very valid business reasons. The problem was that the same identical situation would receive a different code in two different states, thus creating a situation similar to the Relative Value coding structures of long ago.

In its wisdom, HIPAA said "no more" to "local" HCPCS codes. Big turmoil ensued. The payers were legitimately asking how to bill for all those products and services that were being billed with "local" codes. So the National Medicaid EDI HIPAA (NMEH) Workgroup took upon itself to first make an inventory and then see what could be done about the HIPAA mandate of eliminating the "local" codes.

The first inventory of Medicaid "local" codes from only 30 states came up with over 30,000 of them. The first attempt at removing duplications came up with 18,000 codes. Still too many. The NMEH then organized 9 workgroups to work on different code categories. The codes were grouped into 33 categories and distributed to volunteers to organize them and remove redundancies. For example, one group started with 3,000 codes, reducing them first to 300 and finally to just 3 unique codes. Currently, with about 30 of the code workgroups having completed their effort, the expectation is that there will be less than 500 total codes and modifiers that reflect the 30,000 initial codes.

How is this possible? Keep in mind that the old local codes used to reflect changes in provider location, contract terms, and other conditions that were not directly linked to the product or service in the code. If these conditions are coded in the 837, as they should, instead of being coded in the HCPCS code, the HCPCS codes become much simpler. And, then, if the code is the same for the same service across all 50 states, the redundant codes are eliminated.

So, when does the process start? The process started long ago, in January of 2001, and is about ready to finish. Over the last year the CMS National Panel in charge of the HCPCS codes has been issuing new national codes to replace the "local" codes. Many of these new national codes are already part of the 2002 edition of the HCPCS codes. The rest are expected to be released in the first and second quarter of 2002. In a typical year, the HCPCS Level-II codes see about 400-500 changes. The 2002 edition has close to 600 changes. Not a big difference, but most of these changes in the 2002 edition of HCPCS are to issue Level-II codes that replace "local" codes.

Now it is your turn. The CMS HCPCS National Panel has issued national Level-II codes that replace most of the local codes. The process will complete in the next few months. Now payers and providers alike must go over the HCPCS codes they use and determine how to best replace their "local" HCPCS codes with the new national codes. The NMEH is publishing crosswalks to help you with the migration. But you need to do your own conversion.

And, if in the conversion process you find that the HCPCS National Panel missed something, you are welcome to send them your code request. Just make sure there is not a new code for what you need, and make sure there is not another way to encode the product or service in the 837.

Take a look at the Medicaid HIPAA web site, http://www.hcfa.gov/medicaid/hipaa/adminsim/default.htm, for more information on the NMEH local code efforts and other medicaid HIPAA initiatives. Also look at the HCPCS web site, http://www.hcfa.gov/medicare/hcpcs.htm, to see what the HCPCS National Panel is working on and for instructions on how to send in a code request.

And start converting your systems to the new codes that are already in effect. No need to wait for HIPAA to do it!

(Last minute thought. If you want to know about BIPA, keep in mind that BIPA only affects those few HCPCS Level-III codes that were indeed registered with HCFA as national codes. There are so few of them that you can just ignore that part of BIPA as practically irrelevant.)

Kepa Zubeldia, M.D., is President and CEO of Claredi, a leading provider of HIPAA EDI compliance testing and certification. http://www.claredi.com

==========

7 >> H I P A A / SECURE: Security Q/A
"Bare Bones Risk Assessment"
by Eric Maiwald, CISSP

Q: We are a relatively small hospital (100 beds) with a limited budget. What efforts, at the minimum, should be included in our HIPAA technical security risk assessment? As a follow-up question, will this work require outside security consulting expertise?

A: The issue that you face (small organization with a limited budget) is something that we frequently encounter. Since the HIPAA rule will affect a small organization as just as it will affect a large one, it is important for you to identify your areas of non-compliance and correct them.

That being said, it is good practice (even if HIPAA did not exist) for your organization to conduct an assessment and identify potential areas of information security risk. In an assessment, the following areas of your organization would be examined:

* Computers and network technical security measures
* Physical security around computers and networks
* Policies and procedures
* Backups and disaster plans
* Employee awareness
* Employee skill levels and workloads
* The organization's attitude to security
* The organization's adherence to policy

The results of a risk assessment should be a list of potential risk areas and cost effective recommendations for managing the risks (keep in mind that risk can never be completely removed).

If the assessment is to focus on the HIPAA rule, your organization should add

a detailed examination of six key HIPAA areas to the basic assessment. These key areas are:

* Access Control - how the organization prevent unauthorized individuals from accessing sensitive information
* Audit - how the organization tracks activity on systems
* Authorization Control - how the organization gains permission to disclose sensitive information
* Data Authentication - how the organization identifies if information has been modified in an unauthorized manner
* Entity Authentication - how the organization proves that an individual is whom he says he is
* Communication Over Open Networks - how the organization protects sensitive information that is sent over an open network

---

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides enterprise security management services and information security process and monitoring services for healthcare and other industries. http://www.fortrex.com

==========

BRING YOUR HIPAA QUESTIONS AND IDEAS TO LIFE AT...
H I P A A l i v e!

Join nearly 5000 other thinkers, planners, learners and lurkers who are already members of our sister email discussion list. We almost make HIPAA fun! Almost. (Also available in a PREMIUM version of easy-to-navigate, individually formatted, "cleaned up" digests.)
Subscribe now at: http://www.hipaadvisory.com/live/index.htm?tt226

==========

RAISE YOUR ORGANIZATION'S HIPAAWARENESS WITH
H I P A A n o t e s !

Over 9000 subscribers already receive our weekly byte of HIPAA. HIPAAnotes are suitable for publishing on your organization's intranet or newsletter & come free to your emailbox. Subscribe now at:
http://www.hipaadvisory.com/notes/

==========

COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/newsarchives.htm

==========

==========

==========
==========

Switch to HTML or text version at:
http://www.hipaadvisory.com/signup/change.cfm

You are currently subscribed to hipaalert
as: kmckinst@dmhhq.state.ca.us
======
To view the list's archives, change your settings, or UNSUBSCRIBE, go to:
http://lyris.dundee.net/cgi-bin/lyris.pl?enter=hipaalert